Vol.2018-SPT-31 No.16
Vol.2018-EIP-82 No.16
2018/11/2

ブロックチェーンを利用した刑事手続における デジタル証拠の改ざん防止システムについての考察

小坂谷聡[†1]　上原哲太郎[†2]

概要：刑事手続においてデジタル証拠が扱われる際に，しばしばその証拠の収集続きに瑕疵がなかったのか，提出されたデジタル証拠が警察や検察の手によって改ざんされたものではないのか問題となる．そこで、本発表では，ブロックチェーンを用いた証拠改ざん防止しシステムについて提案し，その有効性や実現可能性について考察する．

キーワード：ブロックチェーン，刑事手続き，デジタル証拠，電磁的証拠，改ざん防止

Anti-Tampering System using Blockchain Technology for e-Evidence on Criminal Procedure

SATOSHI KOSAKATANI[†1]　TETSUTARO UEHARA[†2]

1. はじめに

個人や企業等の活動の痕跡として機械的に記録されるデジタルデータを解析することによって得られるデジタル証拠は，客観的・科学的証拠の１つとしてそれ自体高い信頼性が認められており，裁判実務においても重要な証拠として扱われる機会も必然的に多くなっている．

しかし，デジタル証拠は一般に改ざんが容易であるという特性が認められる．その一方，デジタル証拠はその客観的性質ゆえ信頼性が高いと評価される反面，一旦改ざん等された場合には，却って誤判の危険性は増大しその場合の弊害は甚大である．特に，人権問題に直結する刑事裁判では，デジタル証拠の収集保全に関して圧倒的な権限を有する捜査機関が仮にデジタル証拠を改ざんする不正に関与するようなことがあれば，その弊害は計り知れない．手続きの担い手が警察や検察であるということにのみ信頼の基礎を置いていては，国民の信頼に資する裁判の実現には到底及ばない．

以上の理由から，捜査機関によって収集保全されたデジタル証拠に関して，改ざんされていないことが客観的に担保され，かつ弁護人等からも容易に改ざんの有無を確認できるシステムの構築が求められる．我々は，「刑事手続におけるデジタル証拠の改ざん防止措置について」において，押収したデジタル証拠のハッシュ値を特定の第三者機関が管理する中央管理型登録用サーバにアップロードするシステムの構築を提案した．本研究では，上記システムをより信頼性の高い永続的なシステムとするためにさらに考察を進めた．刑事手続におけるデジタル証拠の収集過程について現行法の手続きに沿って概観するとともに，電子公証制度等の既存の制度についての問題点についても検討を加えた．その上で，新たなハッシュ値保管システムとしてブロックチェーン技術について着目し，刑事手続におけるデジタル証拠の収集保全手続において応用するための具体的なシステム構築等について考察した．

†1 立命館大学大学院情報理工学研究科博士後期課程，弁護士
Graduate School of Information Science & Engineering
Ritsumeikan University,　Attorney at Law.
†2 立命館大学情報理工学部
College of Information Science & Engineering Ritsumeikan University

2. 刑事手続におけるデジタル証拠の収集手続について

2.1 証拠の収集手続について

(1) 差押手続きについて

捜査機関が強制処分として証拠物の差押え等を行うためには，令状裁判官から差押えるべき物等を明示した令状（捜索・差押許可状）の発布を受けなければならない．

捜査機関は，上記令状が発布されると捜索すべき場所へ赴き，処分を受ける者に令状を提示するとともに，住居主等を立会人として立会わせることが必要とされている．なお，捜査段階における被疑者の弁護人の立会いは法文上明記されていないことから，弁護人が居住主の代理人である場合を除いては，弁護人の立会いが認められるか否かは実状として捜査機関の裁量に委ねられている．

(2) 差押調書等の作成

捜査機関は，差押え等を行った場合には，（捜索）差押えの日時，場所，目的たる物，立会人，差押えた物，差押え経過について記録した（捜索）差押調書を作成しなければならない．調書には品名や被押収者等の住所，氏名が記録された押収品目録が記載添付される．そして，被押収者に対しては，品名，数量が記載された「押収品目録交付書」が交付される．

Vol.2018-SPT-31 No.16
Vol.2018-EIP-82 No.16
2018/11/2

2.2 デジタル証拠について

(1) 電磁的記録についての手続き

従来，デジタルデータが記録されたオリジナルの記録媒体からデータのみを差押えるという方法は認められていなかった．しかし，デジタルデータそのものだけが必要な場合やオリジナルの記録媒体を差押える必要がない，あるいは差押えることが不都合もしくは困難な状況も存在することから，平成 23 年，刑訴法の一部が改正され，次の３つの場合に，押収すべきデジタルデータに関し，他の記録媒体へ記録させ,その記録媒体を差押えることが可能となった．

①記録命令付差押え（99 条の 2，218 条 1 項）

裁判所が令状発布の際に，電磁的記録を保管する者等に命じて必要な電磁的記録のみを記録媒体に記録等させた上,当該記録媒体を差し押える方法である．

②電磁的記録の複写等（110 条の２,123 条 3 項,222 条 1 項）

差押状の執行をする者が，差押えに代えて，差押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写等した上，当該他の記録媒体を差し押える方法である．

③電気通信回線接続記録の複写（99 条 2 項，218 条 2 項）

差押えるべき物が電子計算機であるときは，当該電子計算機に電気通信回線で接続している記録媒体に保管されており，当該電子計算機で作成・変更・消去することができる電磁的記録については，当該電子計算機等に複写した上，当該電子計算機等を差押える方法である．

(2) 電磁的記録にかかる差押調書等

電磁的記録についても捜索・差押をする場合には，同じく居住主等の立会いが必要であり,差押えた場合には,（捜索）差押調書を作成し，また，押収品目録交付書を交付する．なお，電磁的記録の複写等の処分を行った場合及び電気通信回線接続記録の複写による差押えの場合には，経過を記載する欄にその旨及び経過を記載する．また，記録命令付差押えの場合には，記録命令付差押調書を作成し，記録命令付差押えの日時，場所，立会人，記録等させた電磁的記録，記録等させた者，記録命令付差押えにより差押えた物,記録命令付差押えの経過を記載しなければならない．

2.3 デジタル証拠の改ざん防止措置の必要性

デジタル証拠が適法な証拠たり得るのは，捜査機関によって押収等の過程で偽造や改ざんがなされていないということが保証されていることが前提である．しかし，以下に示す通り，刑事裁判においてデジタル証拠の真正性・完全性が何らかの形であれ問題となった事例も実際に存在し，また，検察官でさえも自ら証拠の改ざんに手を染めた現実を目の当たりにすると，もはや捜査機関であるからと言って全幅の信頼を与えることは出来ないと言う他ない．

(1) 刑事事件においてデジタル証拠の真正性・完全性が問題となった事例

① 改ざん自体が争点となった訳ではないが，検察官によって証拠が改ざんされた，いわゆる厚労省フロッピーディスク改ざん事件として知られる一連の事例がまず挙げられる（大阪地判平成 22 年 9 月 10 日，大阪地判平成 24 年 1 月 23 日，大阪地判平成 23 年 4 月 12 日，大阪高判平成 25 年 9 月 25 日）．この事件は，捜査主任の検察官によって証拠資料である FD のファイルシステム上のメタデータ（最終保存日時）が改ざんされたという事例である．

② また，デジタルデータの改ざんが直接問題となった事例としては，まず，検察官が提出したサーバのアクセスログ（履歴）に対して，弁護人がその改ざんを争った事例がある（東京地判平成 17 年 3 月 25 日（ACCS 事件））．裁判所は，アクセスログの記録が第三者によって不正に作出された「可能性をうかがわせる具体的な事情は何ら存在しない上，第三者が被告人のアクセス記録をことさらに作出する必要性もないことから，アクセスログは正確に被告人のアクセスを記録していると認められる．」と判断した．

その他，被告人と共犯者間の携帯メール等の送受信に関して，共犯者が特殊なソフトウェアを使ってメールのヘッダ情報を書き換え，成り済ましメールを作成した事実があるとして被告人によって争われた事例（さいたま地判平成 21 年 7 月 28 日）や，被告人が証拠として提出した IC レコーダに記録されたデジタル音声データについてその改ざんの有無が争われた事例（高松高判平成 24 年 4 月 26 日）がある．前者の事例では，メールのヘッダ情報の書換えが技術的に可能であるとしても，共犯者が，被告人との間のメールの送受信をわざわざ偽装する理由も必要性も見当たらないとして被告人の主張が退けられた一方，後者の事例では，デジタルデータは痕跡を残さずに加除訂正することが容易であることを認めた上で，やり取りの中には相当不自然な部分もあることを理由に元の音声データに対し加除訂正が加えられたものであると認定されている．

さらに，被告人から提出された写真データに関して，写真データの EXIF 情報が改ざんされた痕跡は特に見当たらないとする捜査機関が実施した鑑定が存在するにもかかわらず,検察官がその改ざんの可能性の有無を争った事例(水戸地判平成２３年５月２０日）が挙げられる．この事例では，裁判所は，当該写真に記録された撮影日時の情報について，人為的に改ざんが行われたことを推認させる具体的形跡等は特に認められないと判断し，検察官の主張を退けた．

(2) デジタル証拠の改ざんリスク

刑事裁判においてデジタル証拠の真正性・完全性が争点化された事例は，我々が調査した限り現時点では件数自体は多くないが，何れにしても，裁判所がその判断基準としているところは，デジタル証拠の改変の容易性ないし危険性というよりは，改変の可能性を疑うに足る具体的な事情の有無によるところが大きいと言える．これは，デジタルデータは改変しやすい性質であるということを一般的な知識としては理解しつつも，現実的な危険性としては十分に

捉え切れていなかったことによると考えられる．しかし，デジタルデータの改ざんは，現在では限られた専門家でなくても容易に扱える技術となりつつあり，それは，捜査官においても同様である．我々は，一捜査官の個人的対応によっても容易にデジタル証拠の改ざんは実行されうる状況にあるという現実に率直に向き合わなければならず，それがゆえに，捜査機関による偽造・改ざんのリスクについても十分に警戒しなければならない．ここに，捜査機関によってデジタル証拠が改ざんされることを防止するための措置が必要であることの理由がある．

(3) ハッシュ値の活用

この点，捜査機関によって収集保全されたデジタルデータの改ざん防止策としては，オリジナル媒体のデジタルデータと同一であることをハッシュ値によって確認することが最も効果的である．捜査機関等がハッシュ値を確実な手段で証拠化しておくことで，同一性あるいは改ざんの有無を確認することができる．弁護人としては，捜査機関が押収したデジタル証拠に関して，ハッシュ値が記録されているかどうかを確認し，仮にこれが同一でなかった場合には，提出されたデジタル証拠の証拠能力や証明力を争うことになる．しかし，問題はそのハッシュ値の確認手段ないし方法である．

ところで，押収すべき電磁的記録が捜査機関によって偽造ないし改ざん等される可能性を考えた場合，（ⅰ）押収される段階と（ⅱ）保管・管理の段階での２つの場面が想定できる．そこで，まず，この２つの場面に分けて，ハッシュ値確認の手段に関する問題について検討する．

2.4 押収段階での改ざんの危険性

(1) 立会人について

捜索・差押えの際に立会人が必要とされているのは，押収段階において，捜査機関が，令状記載の差押対象物（電磁的記録に係る記録媒体）以外の物を差押えていないか，その場に存在しない物を存在したと称して証拠をでっち上げていないか等違法な差押えに対して，差押え場所の管理者として監視の目を光らせ，違法を抑止するための適法性の担保としての機能が期待されているからである．しかし，被疑者の弁護人の立会いが制度的に保障されていない現状においては，立会人が捜索・差押え等の手続きについて法的に精通していることは望めない．その上，住居主等が立会えないときには，「隣人又は地方公共団体の職員」など当該事件とは無関係の第三者の立会いで足り，住居主が不在等や立会いを拒否した場合であっても捜索・差押手続きが出来なくなる事態に陥ることはない．従って，捜査機関による執行の違法性をどれだけチェックできるのかということに関しては自ずと限界がある．特に，電磁的記録に関しては，法的知識以外にも，ハッシュ値についてなど情報処理についての高度な専門的知識や技能が要求され，かかる専門的知識がなければ，電磁的記録に係る記録媒体の差押え等に際して，捜査機関が何を行っているのかということについても簡単には理解できるとは想定できない．

(2) 押収品目録交付書について

違法な差押えを抑止するための手段としては，他に，捜索･差押調書及び押収品目録交付書の作成等が挙げられる．

しかし，ここに記載されるのは，「物」としての押収品である．電磁的記録の場合であれば，押収物そのものは電磁的記録が記録された記録媒体であることから，その記録媒体が記載され，そこに記録されている電磁的記録自体は特に特定され記載が求められている訳ではない．確かに，電磁的記録に関する差押等については，令状の請求に当たって，対象となる電磁的記録ついては一定の特定が必要であり，差押段階においても記録媒体の中身を確認した上で差押えることが必要であることは当然である．しかし，実際に差押えられた記録媒体については，それに格納された電磁的記録まで記載することまでは求められていない．これでは，差押えの対象とされていたオリジナルのデジタルデータが，そのままの状態で複製等されたことについては事後的に確認しようがない．デジタルデータに関しては，前述のハッシュ値の記録が考えられるが，現状においては目録等の記載は義務付けられていない．

2.5 保管・管理段階での改ざんの危険性について

通常の押収物の場合とは異なり，電磁的記録の場合には，仮に，押収段階において適切にハッシュ値が算出・記録されてさえいれば，その後に改ざんされたとしてもその検出は容易であり，保管中の改ざんリスクは減少する．従って，ここでは，差押えられた記録媒体に記録された電磁的記録に関して，差押え時にハッシュ値が計算・記録されていなかった場合について検討することが必要となる．この点，捜査機関からも，記録媒体の解析に際しハッシュ値を計算して記録・保管しておくことが推奨される見解もあり，この手続きが適切に実施されるのであれば，少なくとも，解析時以降のハッシュ値は記録される．しかし，そもそも，差押時ないし実際にハッシュ値が計算されるまでの間に改ざんがなされなかったことについては何の担保もないが，この点は差し置くとしても，この手続きでは，捜査官による関与しかなく，その運用に委ねられている以上，客観性の担保が弱いと言わざるを得ない．いずれにしても，ハッシュ値を記録・確認するための客観的かつ統一的な制度ないしシステムの確立が求められるところである．

3. ハッシュ値の記録先としてのブロックチェーンの利用

捜査機関が押収した電磁的記録が押収時の状態のまま適切に保管・管理され，改ざんされていないことを証明するためには，当該電磁的記録のハッシュ値を記録・確認することが効果的であるとして，それが客観的ないし公的に証

明ないし認証されていなければ十分とは言えない.そこで,ハッシュ値の保存手段として，まず既存の制度を利用することができないか考える.

3.1 電磁的記録に対する存在証明のための制度

(1) 公証制度に基礎を置く電子公証制度

文書等を公的に証明する手段としては，まず，公証人による公証制度の存在が挙げられる．そこで，捜査機関が作成した電磁的記録のハッシュ値についてもこの公証制度を利用することができないか検討する.

公証制度は，従来，紙の文書に限定されていたが，一部の電子的なデータ（電磁的記録）に関しても公証人による公的な証明を施すべく，公証人のうち新たに電子公証事務を行う公証人を指定公証人として創設し公証制度の中に取り入れられることになった．この制度が電子公証制度である．現在，電子公証制度には大きく分けて，①電磁的記録の認証と②日付情報の付与（電子確定日付の付与）の制度がある．このうち②は，指定公証人が電磁的記録に記録された情報に日付を内容とする情報を付し，これに電子署名をすると，当該情報を確定日付のある証書とみなすことができる制度であり（民法施行法 5 条 2 項），文書の存在を証明する制度として利用されることから，この制度を公的なハッシュ値の存在証明として利用することが考えられる.

しかし，公証制度は，私的法律関係の明確化等を図ることを目的とした制度であり，そもそも公務員が作成した文書についての利用を前提としていない．法文上も公務員が職務上作成した電磁的記録以外のものに限定されている（公証人法 1 条 1 項 4 号但書，民法施行法 5 条 2 項但書）．もっとも，公務員が作成ないし管理・保管している書面や電磁的記録であるからと言って，それらが，改ざんのリスクと無関係である訳ではないので，現行制度の枠組みに必ずしも限定されず広く電子公証制度を捉え直すことも立法論としては検討に値する.

(2) 民間のタイムスタンプサービス

では，次に，民間事業者による電子署名を用いたタイムスタンプサービスの利用についてはどうか.

タイムスタンプサービスとは，タイムスタンプ局とよばれる第三者機関が，利用者が持つデジタルデータがある時刻以前に存在したことを証明する技術であるタイムスタンプ技術を利用したサービスである．この制度は，電子署名法に基づいて特定認証業務を行う事業者として認定された認証業者など信頼性の高い民間事業者による電子署名を用いた制度であり，電子公証制度と同じく PKI 制度に基盤を置いた，第三者の電子署名の信頼に基づいた制度である.

このサービスを利用すれば，電磁的記録のハッシュ値を生成した際に，そのハッシュ値をタイムスタンプ局に送信し，タイムスタンプ要求を行えば，タイムスタンプ局において時刻証明となる情報を添付したタイムスタンプ・トークンを生成し，それにタイムスタンプ局のデジタル署名を施して返送されることから，これを元のデータとともに保管しておけば，時刻証明された時刻以前にその内容のデータが存在したということが保証される.

(3) 問題点

電子公証制度をベースとした電子公証システムにせよ民間事業者を利用したタイムスタンプ制度にせよ，これらの制度は，PKI に基盤を置いた制度であり，特定の第三者機関に依存した制度である.

そうすると，まず，これらの制度の前提として，当該対象となる電磁的記録情報は必ず特定の第三者機関等に送信し日付情報やタイムスタンプを付してもらわなければならないことになるが，これは，特定の認証機関ないし限定された指定公証人に負荷が集中するリスクを伴う．サービスを受けたい時に受けられないリスクは否定出来ず，迅速性が求められる捜査段階で期待通りの活用が認められない恐れがある.

また，例えば，タイムスタンプは，タイムスタンプ局の電子署名が施されていることによってその時刻証明が保証されるが，その保証は，電子認証局がタイムスタンプ局に発行した公開鍵証明書の有効期限に当然縛られる．有効期限を越えたデータは検証手段がなく，その有効期限を越えて保証されるためにはタイムスタンプを付し直さなければならない．これは，指定公証人による電子署名においても同様である．従って，これらの制度では情報を長期的・永続的に保存することに限界がある.

さらに，電子公証制度においても，タイムスタンプ制度においても，情報の同一性を証明した電磁的記録やタイムスタンプが付された情報を公開する場所や手段がないということである．タイムスタンプが付されたデジタルデータ（電磁的記録のハッシュ値）は，利用者の手元に保管されているだけであり，タイムスタンプ局が，時刻証明となる情報を一元的かつ集中的に管理・公開する訳ではない.

なお，電子公証制度において利用者が日付情報の付与を受けた電磁的記録と情報の同一性に関する証明を請求するためには（また，タイムスタンプ制度においても，申請の際，利用者による電子署名を要求するなら），電子署名（電子証明書の取得）が必要とされている（なお，現行法上，日付情報の付与の請求自体に関しては，当該電磁的記録に電子署名を付与する必要はない.）．しかし，押収された電磁的記録のハッシュ値保全システムにおける利用を考えた場合，直接的な利用が想定される警察官や検察官においては，例えば官職証明書を利用するなどの方法が考えられるが，それに代わる制度のない弁護人にとっては利用しづらい制度となる．司法書士など多くの士業においては，司法書士会等各業界団体が主導して民間業者等を利用した職業上の電子証明書が付与されるシステムが既に構築されている．しかし，弁護士が「弁護人」ないし「代理人」として業務を行う上での同様のシステムは存在せず，弁護士が電

子証明書を利用するには，新たに，PKI に基盤を置いた弁護士認証システムのような仕組みを構築する以外には，現状では，各弁護士が個人として電子証明書を作成するか，あるいは，同じく個人として公的個人認証サービスを利用するなどしか方法がない．

3.2 ブロックチェーンを利用する意義

そこで，特定の機関に過度に負荷が集中せず可用性が保証され，さらに，誰でも，そしていつでも情報を確認することができ，しかも半永久的に保存可能なシステムとして，ブロックチェーンを利用するシステムについて検討する．

ブロックチェーンとは，データベース全てをネットワーク参加者（ノード）全員が分散して共有し，そのデータの正当性を相互に保証する分散型台帳システムである．ブロックチェーンでは，ネットワークに送信された各データ（電磁的記録のハッシュ値）が複数纏められその全体のハッシュ値と一つ前のブロック全体のハッシュ値等から次のブロックが形成されるようにして，ブロックのチェーンが形成される仕組みとなっている．そのため，一旦格納されたデータに関して，１つのノードで改ざんがあれば，ネットワークの全ノード間での整合性が保てなくなることから，データの改ざんは極めて困難となる．また，従来の技術は，特定の事業者や機関など中央集権的にデータを管理する機関の存在が前提とされていたが，ブロックチェーンでは，ネットワークに参加する全ノード間の相互の監視機能を以てデータの真正性を担保している．従って，その特定の機関が十分に信頼に足りる場合には敢えてブロックチェーンを利用しなければならない必要性は乏しいかもしれない．しかし，この場合でも，特定の機関に負荷が集中するリスクは避けられない．また，そもそもその特定の機関に対する信頼関係を前提におけない場合，例えば，デジタル証拠を収集保管する捜査機関に対して根強い不信感から信用性を客観的に担保する制度が必要であると考える立場を前提とすれば，第三者機関であったとしても捜査機関の関与が強くうかがわれる機関であれば意味がない．このような疑念を払拭して弁護人からも信頼できるシステムを構築する上でも，非中央集権的な管理の仕組みを持つブロックチェーンを利用する意義は十分見出せる．

4. ブロックチェーンを利用したハッシュ値保全システムの検討

ハッシュ値保存システムとして，新たにブロックチェーンを利用したシステムの可能性について指摘したが，具体的にどのようなシステムが適しているか検討する．

4.1 ブロックチェーンの種類

ブロックチェーンには，大きく分けて(ⅰ)アンパーミッションド型（パーミッションレス型）と(ⅱ)パーミッションド型が存在する．前者(ⅰ)は，ビットコインやイーサリアム等に代表される中央の管理者を必要とせず，ネットワークへの参加について制限を設けない自由で開かれたシステムである．このシステムにおいては，利用者の身元確認は必須ではなく，台帳に書き込まれたデータは誰でも閲覧・参照が可能であるとされる．これに対して，システムに接続し台帳のデータを書き込んだり，閲覧・参照が出来る利用者を一定の資格を有する者に制限したいという要請から，システムへの参加要請等に対して，単独ないし複数の管理者によるシステム許可ないし承認を必要とするものが後者(ⅱ)である．

4.2 ハッシュ値保全システムにとってのブロックチェーンとは

では，ハッシュ値保全システムを構築するにあたってはどのタイプのブロックチェーンの利用が適しているか．

分散型台帳に保全されるデータは，捜査機関が押収した電磁的証拠のハッシュ値であることや台帳に書き込まれたデータを参照・確認するニーズを有している者は弁護人や被疑者・被告人，被押収者等の当事者，あるいは捜査機関や検察等に限られる．また，台帳に書き込むことが想定されている主体も捜索押収の実施主体である捜査機関に限られている．これらのことを考えると，広くシステムの利用を一般に開放する必要性は乏しく，パーミッションド型の方が適していると考えることも出来る．

もっとも，台帳に記録されるデータは，電磁的証拠それ自体ではなく，あくまでもそのハッシュ値であり，その値自体には特別な意味はない．また，押収された電磁的記録のハッシュ値の保全を目的としたシステムの構築を検討しているが，翻って考えてみれば，民事・刑事を問わず，訴訟において利用されるデジタル証拠一般に広く応用可能であると言える．そうすると，必ずしも，システムの利用者を捜査機関や法曹関係者に限定しなければならない理由も薄い．実際，改ざんの有無を検証するためのハッシュ値情報の開示は，広く一般に公開されている方がより客観的であり，かつ信頼性も高い．また，逆に，ブロックチェーンのネットワークへのデータの送信（書き込み）に関しても，利用者を限定しない場合の弊害はさほど大きくないと考える．確かに，ブロックチェーンの利用者を限定せず広く一般に開放した場合，無関係な情報が溜まっていく可能性は否定できず，また，制度に便乗し私的な利用が横行したり，ひたすらブロックを生成したりする攻撃にさらされるリスクも高まるかもしれない．しかし，ブロックチェーンにおける信頼の源泉は，ブロックチェーンのネットワークにより多くのノードが参加し，ブロックが長く続いていくことによる耐改ざん性にある．とすれば，出来るだけ多くの参加者に利用されることによってもたらされるメリットも無視できない．

以上の点を勘案して，我々は，パブリックなシステムとして検討した場合のメリットを重視して，基本としてアン

パーミッションドなブロックチェーンの枠組みを利用することによって，システム利用者に対する参加制限等は特に設けないものの，他方，ネットワークを確実に稼働させる上で必要となるマイナーとなりうる特定のノード（フルノード）を複数設置してブロックチェーンネットワークで結ぶシステムの構築を提案する．

4.3 電子署名

ブロックチェーンを利用する際にはユーザはアカウントを作成しなければならないが，利用者に限定がなく自由に参加出来るアンパーミッションドなブロックチェーンの場合，このアカウントは任意に作成出来ることが一般的である．アカウントの作成には，秘密鍵と公開鍵の鍵ペアを生成し，この公開鍵をハッシュ化する等の方法による．また，ここで生成された秘密鍵は，ユーザがトランザクションを発行する際に，トランザクションの内容が不当に改ざんされないように署名を行う際にも使用される．

ところで，アンパーミッションドなブロックチェーンにおいて使用される秘密鍵と公開鍵のペアは，PKI とは基本的に異なるものである．PKI においては，秘密鍵と公開鍵を所有する者を信頼される第三者機関（認証局）が証明する仕組みであるが，特定の機関によって管理されていないアンパーミッションドなブロックチェーンにおいては，単に公開鍵やアドレスによってのみユーザが識別され，それが実際は誰なのかはブロックチェーン内部の仕組みからは確認出来ない．従って，ユーザが電子署名を行ったとしても，そのユーザが誰なのかは分からない．利用者を制限せずに誰でも利用出来るシステムの構築を検討するにしても，ブロックチェーンへの情報の登録者が全く誰かも分からないのではシステムの利用に支障が生じ得る．従って，ユーザ確認のための手段についての検討が必要となる．

4.4 利用者確認手段の検討

まず，ユーザ確認の手段に限定して PKI ないし類似の仕組みを利用することは出来ないか．この点，捜査機関に関しては官職証明書の利用が可能であるが，弁護士に関しては，弁護士 PKI のようなシステムが存在していないことは前述した通りである．従って，利用者確認の手段として PKI ないし類似の仕組みを適用し，かつ，利用者として，捜査機関関係者だけではなく，広く弁護士に対しても開こうとするなら，弁護士 PKI のようなシステムを新たに構築することが必要となる．具体的には，例えば，登録弁護士に関して，登録身分証として IC カードを新たに発行し，そこに秘密鍵と公開鍵の鍵ペアを登録し，日弁連あるいは各単位会において，誰にどの鍵ペアを配布したのかという情報として，各登録弁護士の公開鍵を登録番号等から検索出来るように開示する方法が考えられる．しかし，新たな弁護士 PKI システムの構築をブロックチェーンによるデジタル証拠保全システムの前提とすることについては，実現に向けての不確定な要素が大きく，必ずしも適切とは言えない．

そこで，利用者が，ブロックチェーン上で初めに鍵ペアを生成した際に，生成されたアカウント（アドレス）を所属機関に届け出て，氏名，所属，登録番号等から検索出来るシステムをウェブサイト上に開示する等の制度が考えられる．但し，この方法では，登録する際に，なりすましや名義貸し等のリスクは避けられない．しかしながら，弁護士等が上記登録に際して，弁護士会等の所属機関が利用者の身分を確認することは容易であることから，上記リスクは最低限に抑えられると考える．

5. イーサリアムを利用したハッシュ値保全システムの提案

5.1 イーサリアムネットワークの利用

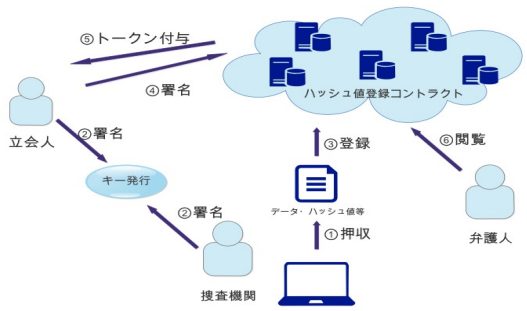
以上の検討を踏まえて，ブロックチェーンを利用したハッシュ値保全システムをアンパーミッションドなブロックチェーンのネットワーク上で実行させるプラットフォームとして，我々は，実装の容易性を考慮してイーサリアムネットワークを利用する．イーサリアムは，暗号通貨の分野では Ether と呼ばれる暗号通貨として，ビットコインに次ぐ市場規模を有しているが，本来的には，単なる暗号通過としての基盤としてだけではなく，スマートコントラクトと呼ばれるブロックチェーン上で実行する任意の自動プログラムのプラットフォームとして開発されたものであり，現在も開発が継続している実績のあるプラットフォームである．

イーサリアムのネットワーク上では，ブロックチェーン上に実現したい各種のスマートコントラクトを格納し，ノード間で実行・共有することが可能であるが，そのスマートコントラクトを実行するためのコストとして，Gas と呼ばれる手数料が Ether を利用して支払われる．また，スマートコントラクトは，１６０ビットのアドレスで表示されるアカウントと呼ばれる概念で管理される．アカウントには，イーサリアムを利用するユーザが保持する外部所有アカウント（EOA : Externally Owned Account）とスマートコントラクトを表すコントラクトアカウント（CA）の２種類がある．外部所有アカウントは，秘密鍵によって管理されたアカウントであり，Ether を送金するトランザクションやスマートコントラクトを実行するトランザクションを発行する際にそのトランザクションに秘密鍵で電子署名を付すことでトランザクションの発行が認証される．そして，コントラクトアカウントは，スマートコントラクトをブロックチェーンにデプロイした際に外部所有アカウントからトランザクションを介して生成されるアカウントとしてブロックチェーン上に存在し，外部所有アカウントが発行するトランザクションをトリガーにスマートコントラクトに記述されたコードを実行する．但し，外部所有アカウントとは異なり，秘密鍵は持たない．

Vol.2018-SPT-31 No.16
Vol.2018-EIP-82 No.16
2018/11/2

5.2 システムの概要

イーサリアムネットワークを利用した提案システムの概要ないし手順等は以下の図の通りである．



図．ハッシュ値登録システムの概要

(1) ハッシュ値登録システムの概要

① マイナーノードの設置

ネットワークを確実に稼働させる上で，マイナーとなる特定のノードを複数設置する．この点，弁護人からも信頼出来るシステムを構築するという観点から，例えば，まず全国 52 の各単位弁護士会ごとに設置することも 1 つの方法である．ノードを局地的に偏在させることなく，また，全国的に一定のノード数を確保することが可能となる．なお，マイナーは，後述する通り，押収手続きの立会人にインセンティブとして付与されるトークンの発行主体となる．

② システム利用者

このシステムではハッシュ値情報を登録し，閲覧する利用者として捜査機関や弁護士を想定している．主たるユースケースとしては，刑事事件において，捜査機関が情報を登録し弁護人が閲覧するケースを想定するが，弁護人が登録し，捜査機関に閲覧させるケースもある（なお，民事事件において，弁護士同士が利用することもできる.）．

③ 登録情報

捜査機関は，原則として電磁的記録の押収時，それができない場合には後日解析時に押収した電磁的記録のハッシュ値を作成する．そして，ブロックチェーン上に実装された登録システムに対して，登録しようとする電磁的記録自体のハッシュ値，及び当該電磁的記録のデータサイズ（bit 単位）などの情報を，後述するランダムな一意な数値とともに登録する．

④ 立会人による手続き担保とインセンティブの付与

捜査機関は，押収手続きが終了すると手続きの開始及び終了日時などの情報をもとにして当該手続きに対して一意となるランダムな数値（K :「キー」と呼ぶ.）を生成する．そして，このキーを押収手続きの立会人と共有及び確認するために，立会人と捜査責任者が各々電子署名（マルチシグ）を施せば，キーのハッシュ値が算出され，ブロックチェーンに登録される．そして，立会人は，捜査機関によって電磁的記録のハッシュ値等の情報をブロックチェーンに登録されたことを確認すると，ブロックチェーンを通じてこれを承認する（電子署名を施す）．この承認行為は，キーを確認し署名した立会人以外は行えない仕組みとすることで, 立会人が, 押収手続きの現場にいたことの証明となり，押収手続きの適法性の担保の一つと成り得る．また，立会人がキーを確認するための電子署名を行うことなどのインセンティブを得るために，立会人の承認終了後には，それに応じて一定数のトークンが当該立会人に付与される仕組みとする．

なお，捜査機関が，電磁的記録の押収時に直ちに電磁的記録のハッシュ値情報を登録することが保証されているのであれば，立会人は立会現場で 1 度電子署名を施せば済むことであって，上記のような二重の承遠手段を取る必要はない．しかし，電磁的記録のハッシュ値情報は押収手続きの現場で算出されることが原則となるべきではあるが，押収現場での手続きの実態を鑑みれば，むしろ後日解析の場面で取られることが少なからずありうると考えられる．従って，このような場合も想定し，立会人の承認行為をもって一連の手続きを終了させることで，捜査機関の速やかな登録行為を促すこととした．

⑤ 登録利用者の外部所有アカウントの公開

一定の機関，例えば，各単位弁護士会等において，システムのコントラクトアドレス，システム利用者がシステム利用時に生成した外部所有アカウントを保存・公開するサーバを設置する．システム利用者は，システムを利用する際，このコントラクトアカウント宛に登録トランザクションを生成する．利用後，公開鍵から生成された外部所有アカウントを登録する．

⑥ ハッシュ値等の記録・開示

登録されるハッシュ値やその他必要な情報については，登録トランザクションの作成時に生成されたトランザクション ID（トランザクションハッシュ）とともに押収品目録ないし弁護人に証拠開示される際に作成される開示証拠目録等に記載する．弁護人は，開示されたトランザクション ID をもとにブロックチェーン上に格納されたハッシュ値等の情報及びトランザクションがブロックチェーンに取り込まれた日時について取得することが可能となる．

(2) スマートコントラクトを利用した処理

ネットワークの参加者がシステムを利用するためのプログラムコードを次の 4 つの機能を有するスマートコントラクトとしてブロックチェーンネットワークに登録する．

① 生成されたキーを共有・確認するために，立会人及び捜査官がマルチシグ方式によって電子署名を行い，キーのハッシュ値を取得する．

② 利用者が，登録しようとする電磁的記録のハッシュ値を生成すると，そのハッシュ値に加え，当該電磁的記録の

データサイズ（bit 単位）を，前述のキー情報に関連付けて登録する．

③　電磁的記録のハッシュ値等がブロックチェーン上に登録されたことを確認すると，立会人はブロックチェーン上で承認（署名）し，それに対してトークンが付与される．

④　利用者は，登録された電磁的記録のハッシュ値等の情報についてキー情報等をもとに参照する．

(3)　その他の処理について

①　ハッシュ値等の生成

システムを利用する捜査機関や弁護士等は，登録しようとする情報(電磁的記録のハッシュ値情報等)を生成する．電磁的記録のハッシュ値を算出するためのハッシュアルゴリズムは，捜査機関が一般的に使用している SHA-256 を採用する．ハッシュ値は，原則として，押収時にハードディスク等の電磁的記録媒体に記録された電磁的記録を他の記録媒体に複写する際，あるいは一旦押収した電磁的記録媒体を解析する際に生成される．なお，データ自体ではなく記録媒体自体に対してハッシュ値を取る場合，ハッシュ値を取る対象となるデータについて，媒体のデータのみを対象とするのか，媒体のメタデータを含むのかについては，予め合意を形成しておくか，前述の証拠開示の際に別途通知する等して弁護人らに開示する．

電磁的記録のハッシュ値等の登録情報を，QR コード等を利用してスマートコントラクトの変数として入力するためのウォレットアプリ等を作成する．

②　電子署名用の鍵ペアの生成

登録トランザクションを実行する利用者がシステム利用時にウォレットアプリ等によって自由に生成する．但し，特定の公開鍵の利用者が推測されるリスクを防止するために 1 人につき 1 つの鍵ペアに限定（固定化）することはせずに，手続きごとに変更する．また，固定化しないことで，秘密鍵を紛失した場合のリスクも最小限に抑えることが可能となる．また，立会人がキーを確認する際や登録の承認の際に行う署名などに使用する秘密鍵についてもウォレットアプリ等を利用して手続きごとに作成する．

③　署名

システムの利用は，原則として，捜査機関や弁護士等を想定しているが，その他一般の利用を特に排除することはせず，利用しようと思えば誰でも自由に利用することは可能とする．利用者は，登録トランザクションを生成しブロックチェーンネットワークに送信する際に，当該利用者が利用時に作成した秘密鍵で署名する．立会人の署名も同様である．

④　キー情報の登録通知

ハッシュ値等の情報とキー情報がブロックチェーン上に登録された際に，その登録されたという情報をキーに署名した立会人に対して通知する．

6. まとめ

本研究では，改ざんが可能かつ容易なデジタル証拠（電磁的証拠）について，特に捜査機関による押収後の改ざんの疑念を払拭させ，国民に信頼される裁判に資するための客観的なデジタル証拠の改ざん防止システムとして，高い改ざん耐性を持つことが認められているブロックチェーンを利用するシステムの有効性を示した．確かに，ブロックチェーン技術については，未だ発展途上の技術であり，システムが不具合なく動き続けるかどうかということについての検証は不可欠である．また，提案システムは，押収されたデジタル証拠自体の改ざんを不可能にするようなシステムでも，また，証拠自体から改ざんの痕跡を発見するシステムでもない．あくまでも，デジタル証拠の押収後に仮に改ざんした事実があればその事実を検出するためのシステムである．従って，捜査機関が電磁的証拠の押収手続きの実施後出来るだけ速やかに利用すればするほど捜査機関による押収証拠の改ざんの疑念は大幅に減少すると言える．押収手続きと同時に押収した全ての電磁的記録のハッシュ値を取り，登録することができれば，その有効性・信頼性は一段と高まる．しかし，デジタル証拠の重要性が増すに比例して押収されるデジタル証拠の情報量等も膨大になっていけばいくほど，デジタル証拠の取扱いに対する捜査機関の実際の運用としては，押収手続きから解析・ハッシュ値登録段階に至るまでの時間はむしろ長くなっていくことが容易に予想される．そうすると，捜査機関が提案システムを利用したとしても，デジタル証拠の改ざん防止に対する効果は限定的とならざるを得ない．もっとも，このような場合については，訴訟の場において，押収手続きの日時から実際にハッシュ値を登録した日時までの時間，あるいはそれだけの時間を要した理由の有無ないし理由の合理性等を検証して，改ざんの可能性の有無を判断する合理的な根拠を抽出する実務を積み重ねていくほかない．そして，最終的には，運用ないし立法，及び技術的な進展によって，押収と同時にハッシュ値を計算して登録可能なシステムの実現が目標となろう．

参考文献

[1] 小坂谷聡，上原哲太郎．刑事手続におけるデジタル証拠の改ざん防止措置について（DICCOMO2017）．
[2] 田篭照博. 堅牢なスマートコントラクト開発のためのブロックチェーン技術入門. 技術評論社, 2017.
[3] 加嵜長門, 篠原航. ブロックチェーンアプリケーション開発の教科書. マイナビ出版, 2018.
[4] セコム株式会社 IS 研究所, NEC 編. ブロックチェーン技術の教科書. C&R 研究所,2018.
[5] 岸上順一, 藤村滋他. ブロックチェーン技術入門. 森北出版,2017.
[6] 松本裕, 倉持俊宏, 山口貴亮. 捜索・差押えハンドブック． 立花書房,2017(3 刷).